

Passkeys: Die Zukunft der sicheren Anmeldung

Passkeys sind eine neue und innovative Methode zur sicheren Anmeldung bei Apps und Websites. Sie bieten im Vergleich zu herkömmlichen Passwörtern eine deutlich höhere Sicherheit und sind dabei gleichzeitig einfacher zu verwenden.

Was sind Passkeys?

Stellen Sie sich Passkeys als digitale Schlüssel vor, die auf Ihrem Gerät gespeichert werden – sei es Ihr Smartphone, Tablet oder Computer. Anstatt sich ein komplexes Passwort merken zu müssen, authentifizieren Sie sich mit Ihrem Gerät selbst, z.B. per Fingerabdruck, Gesichtserkennung (Face ID) oder Geräte-PIN. Der Passkey bestätigt dann im Hintergrund Ihre Identität.

Wie funktionieren Passkeys?

Passkeys basieren auf der WebAuthn-Technologie, einem offenen Standard für sichere Authentifizierung. Wenn Sie sich mit einem Passkey anmelden, findet ein sicherer Austausch von kryptografischen Schlüsseln zwischen Ihrem Gerät und dem Dienst statt, bei dem Sie sich anmelden möchten. Dabei werden *keine* Passwörter über das Internet übertragen oder auf Servern gespeichert.

Die Vorteile von Passkeys gegenüber Passwörtern

- **Höhere Sicherheit:** Passkeys sind deutlich sicherer als Passwörter, da sie nicht gestohlen, erraten oder durch Phishing-Angriffe erbeutet werden können. Sie sind an Ihr Gerät gebunden und erfordern in der Regel eine biometrische Authentifizierung, was einen zusätzlichen Schutz bietet.
- **Kein Merken von Passwörtern:** Sie müssen sich keine komplexen Passwörter mehr merken oder diese verwalten. Die Authentifizierung erfolgt bequem und schnell über Ihr Gerät.
- **Schutz vor Phishing:** Da keine Passwörter übertragen werden, sind Sie vor Phishing-Angriffen geschützt, bei denen Betrüger versuchen, Ihre Passwörter abzufangen.

- **Einfache Nutzung auf verschiedenen Geräten:** Passkeys können über iCloud Keychain (Apple) oder Google Password Manager (Google) sicher zwischen Ihren Geräten synchronisiert werden, sodass Sie sich überall bequem anmelden können.

Passkeys im Vergleich zu Apple-ID/Google-ID

Sowohl Passkeys als auch die Anmeldung mit Apple-ID/Google-ID bieten eine komfortable und sichere Möglichkeit zur Anmeldung. Es gibt jedoch einige wichtige Unterschiede:

Merkmal	Passkeys	Apple-ID/Google-ID
Unabhängigkeit vom Anbieter	Unabhängig von einem bestimmten Anbieter. Funktioniert mit verschiedenen Diensten.	Abhängig vom jeweiligen Anbieter (Apple oder Google).
Gerätebindung	An das Gerät gebunden, kann aber über iCloud Keychain/Google Password Manager synchronisiert werden.	An das jeweilige Konto (Apple-ID oder Google-ID) gebunden.
Schutz vor Phishing	Bietet sehr guten Schutz vor Phishing.	Bietet Schutz vor Phishing, aber die Sicherheit hängt auch von der Sicherheit des Kontos ab.
Wiederherstellung bei Verlust	Bei Geräteverlust müssen die Passkeys über die Synchronisierung (iCloud/Google) wiederhergestellt werden.	Bei Verlust des Kontos muss das Konto wiederhergestellt werden (z.B. per Wiederherstellungs-E-Mail).
Zusätzliche Sicherheit	Kann mit zusätzlichen Sicherheitsmaßnahmen wie Hardware-Sicherheitsschlüsseln kombiniert werden.	Kann mit Zwei-Faktor-Authentifizierung (2FA) zusätzlich gesichert werden.

Vorteile der Nutzung von Apple-ID/Google-ID

- **Bequeme Anmeldung:** Die Anmeldung erfolgt schnell und unkompliziert mit Ihren bestehenden Kontodaten.
- **Single Sign-On (SSO):** Sie können sich mit Ihrer Apple-ID/Google-ID bei verschiedenen Apps und Websites anmelden, ohne jedes Mal neue Konten erstellen zu müssen.
- **Integration in das Ökosystem:** Die Nutzung ist nahtlos in das jeweilige Ökosystem (Apple oder Google) integriert.

Fazit

Passkeys stellen eine deutliche Verbesserung gegenüber herkömmlichen Passwörtern dar und bieten ein Höchstmaß an Sicherheit und Benutzerfreundlichkeit. Die Anmeldung mit Apple-ID/Google-ID bietet ebenfalls Vorteile in Bezug auf Komfort und Integration. Beide Methoden tragen dazu bei, Ihre Online-Sicherheit zu erhöhen. In unserer App unterstützen wir sowohl Passkeys als auch zukünftig die Anmeldung mit Apple-ID/Google-ID, um Ihnen die bestmögliche Erfahrung zu bieten.

Version #2

Erstellt: 17 Januar 2025 18:27:46

Zuletzt aktualisiert: 21 Januar 2025 12:49:28